

Public Safety Working Group (PSWG)

23 October 2018

Lauren Kapin (US FTC)
Co-Chair

ICANN63 GAC Plenary Meeting

ICANN | GAC
Governmental Advisory Committee



1. Introduction and Review of PSWG Activities
2. WHOIS Compliance with GDPR: Impact of ICANN's Temporary Specification on Law Enforcement
3. DNS Abuse Mitigation: update on Domain Abuse Activity Reporting (DAAR) by ICANN (John Crain, ICANN)

1. Introduction and Review of PSWG Activities
2. WHOIS Compliance with GDPR: Impact of ICANN's Temporary Specification on Law Enforcement
3. DNS Abuse Mitigation: update on Domain Abuse Activity Reporting (DAAR) by ICANN (John Crain, ICANN)

Strategic Goals:

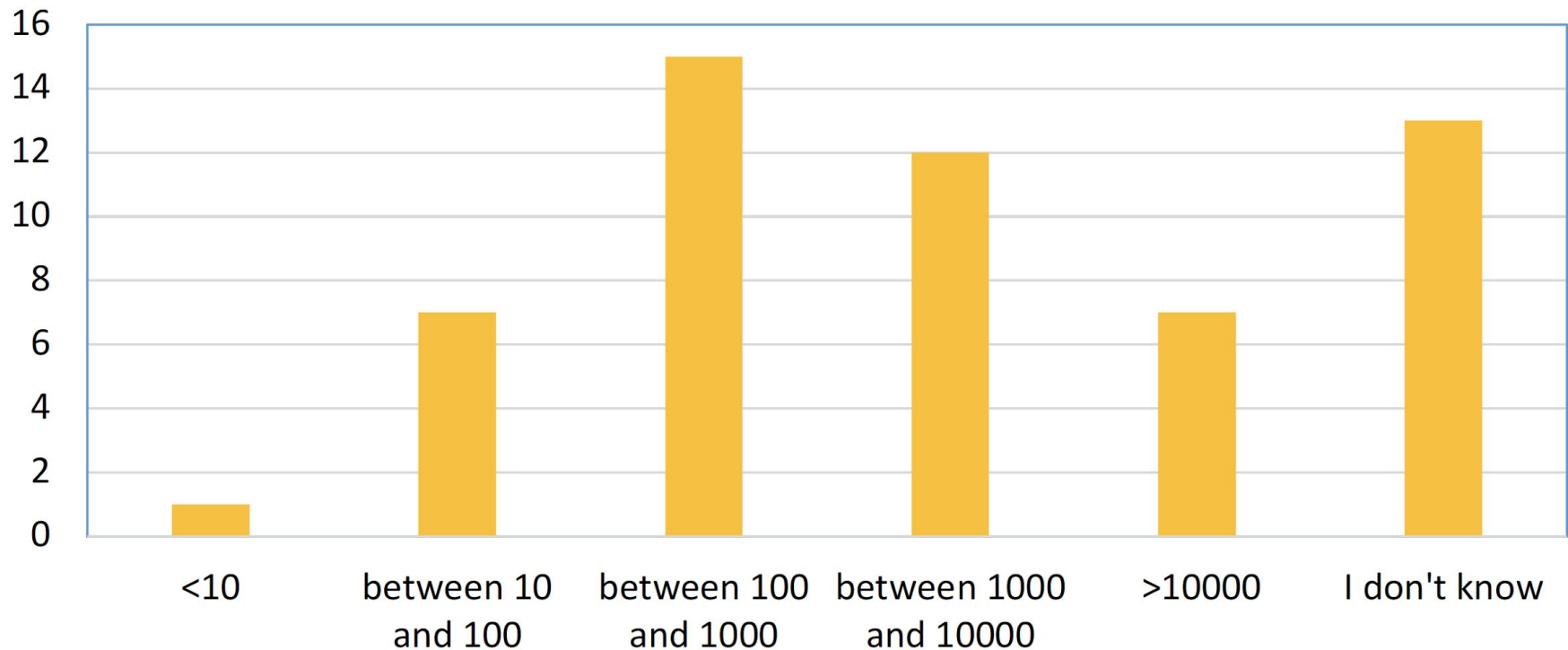
1. Develop DNS Abuse and Cybercrime mitigation capabilities
2. Preserve and Improve Domain Registration Directory Service Effectiveness
3. Build Effective and Resilient PSWG Operations
4. Develop Participation in PSWG Work and Ensure Stakeholder Input

1. Introduction and Review of PSWG Activities
2. WHOIS Compliance with GDPR: Impact of ICANN's Temporary Specification on Law Enforcement
3. DNS Abuse Mitigation: update on Domain Abuse Activity Reporting (DAAR) by ICANN (John Crain, ICANN)

- The WHOIS/RDS2 Review Team conducted a survey of Law Enforcement agencies worldwide
- Goal:
 - to find out more about their use of the WHOIS,
 - to determine whether WHOIS met their investigative needs,
 - to provide a first assessment of the impact of changes made to the WHOIS by the Temporary Specifications adopted by the ICANN Board on 17 May 2018.
- 55 respondents (many on behalf of countries):
Australia, Austria, Bahrain, Belgium, Brazil, Chile, China, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hong Kong, India, Iran, Ireland, Italy, Japan, Kenya, Korea (South), Kuwait, Latvia, Mexico, Morocco, Nigeria, Philippines, Singapore, Slovakia, Slovenia, Sweden, Taiwan, Trinidad and Tobago, United Kingdom, United States of America and Zambia

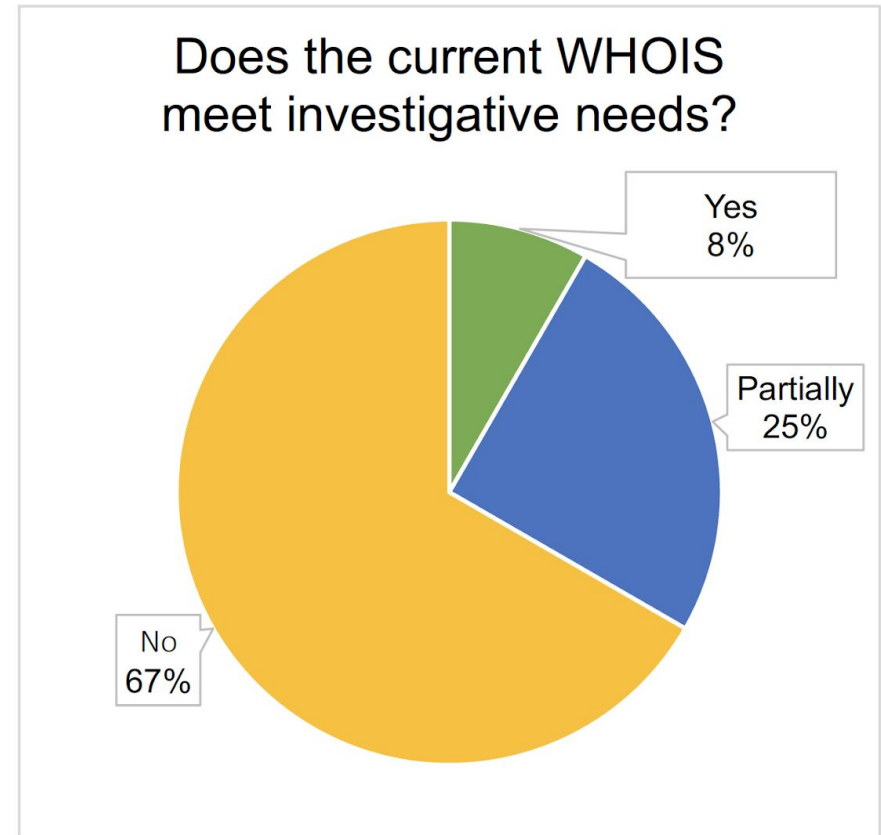
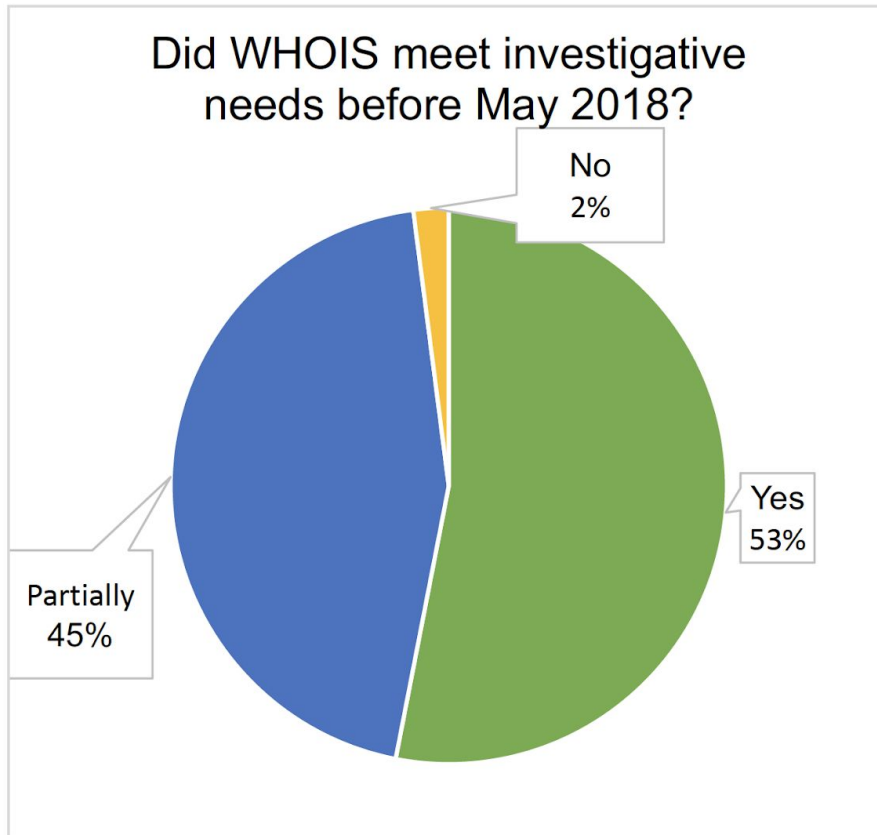
Frequency of Use

Prior to May 2018, how many lookups did your unit or other units or agencies in your jurisdiction whose use you are aware of make?



Source: WHOIS-RDS2 Review Team Initial Report [Webinar](#), 17 September 2018

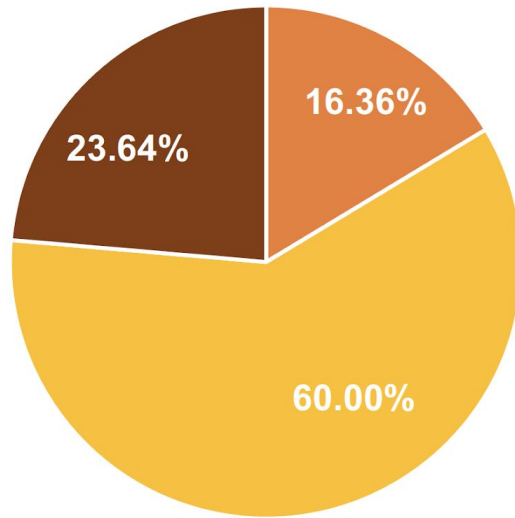
Impact of Change



Source: WHOIS-RDS2 Review Team Initial Report [Webinar](#), 17 September 2018

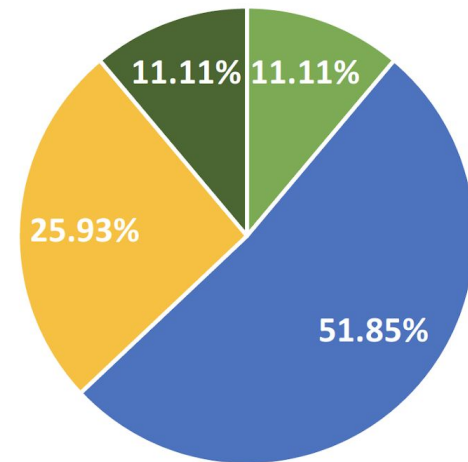
Impact of Unavailability

Are there alternative data sources that you could use or already use to fulfill the same investigative needs?



■ Yes ■ No ■ I don't know

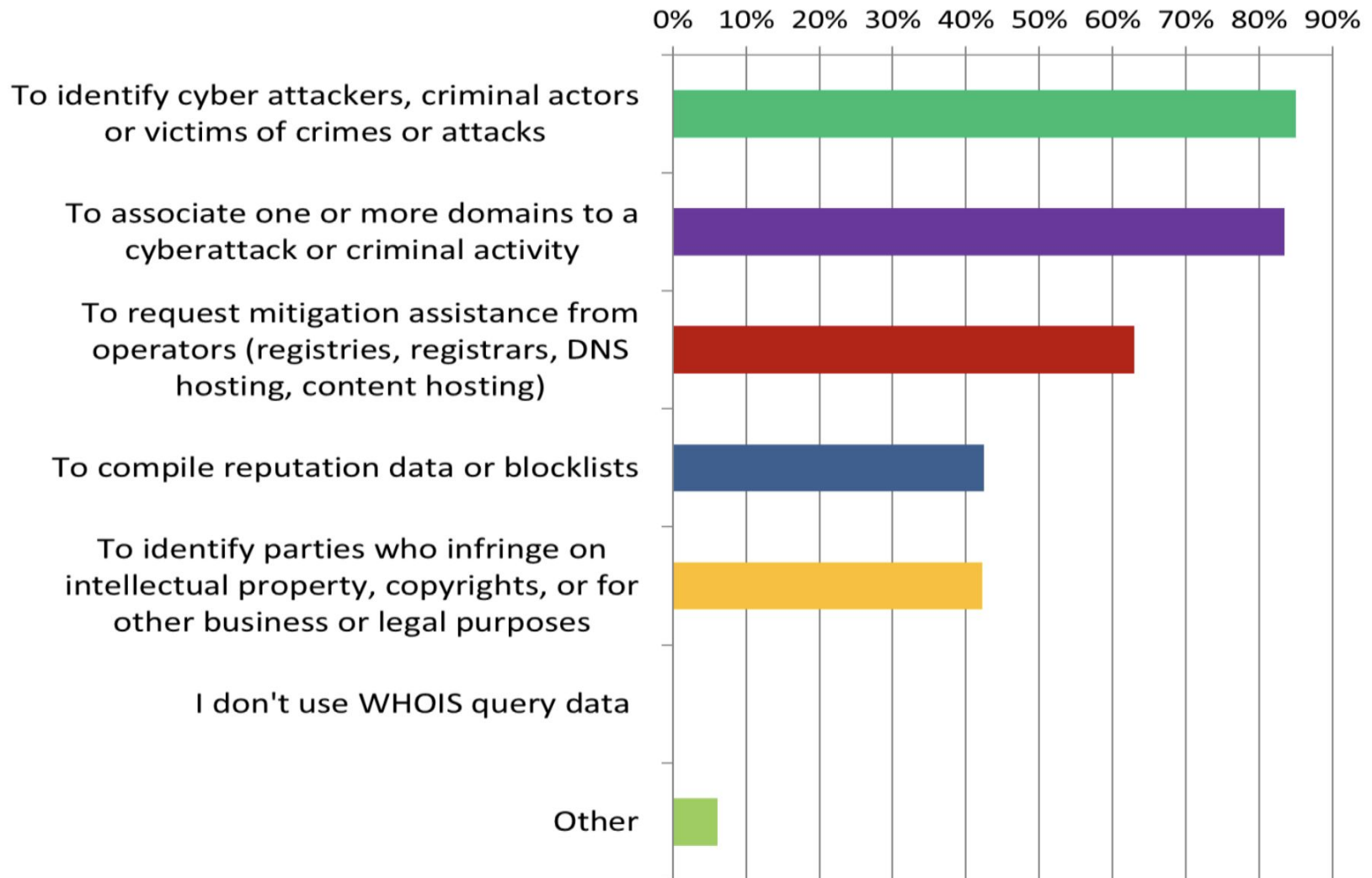
Impact of unavailability of WHOIS information on an investigation



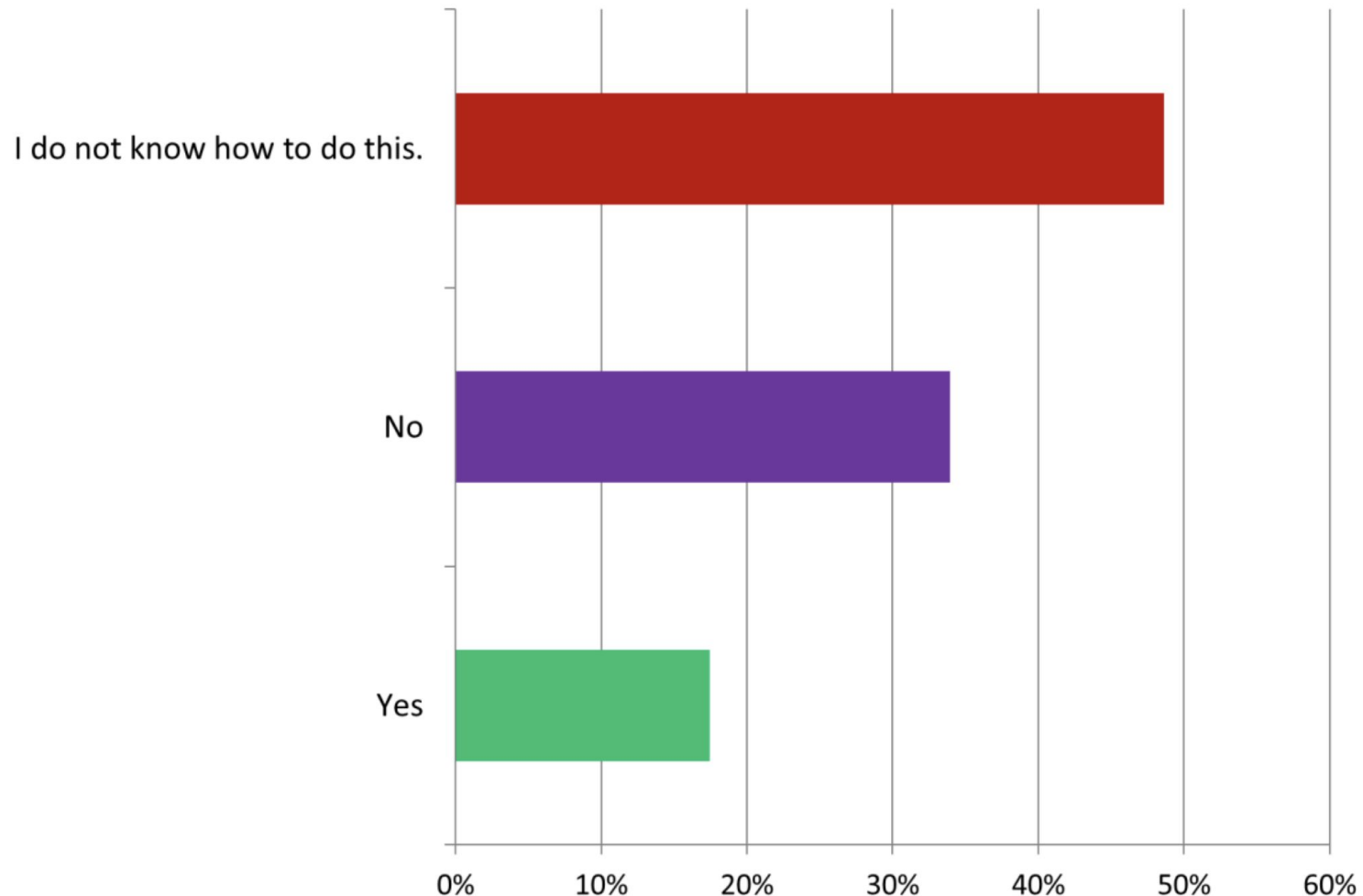
■ Other means are pursued
■ The investigation is delayed
■ The investigation is discontinued
■ Other (please explain)

Source: WHOIS-RDS2 Review Team Initial Report [Webinar](#), 17 September 2018

How do you use WHOIS query data? (choose all that apply)

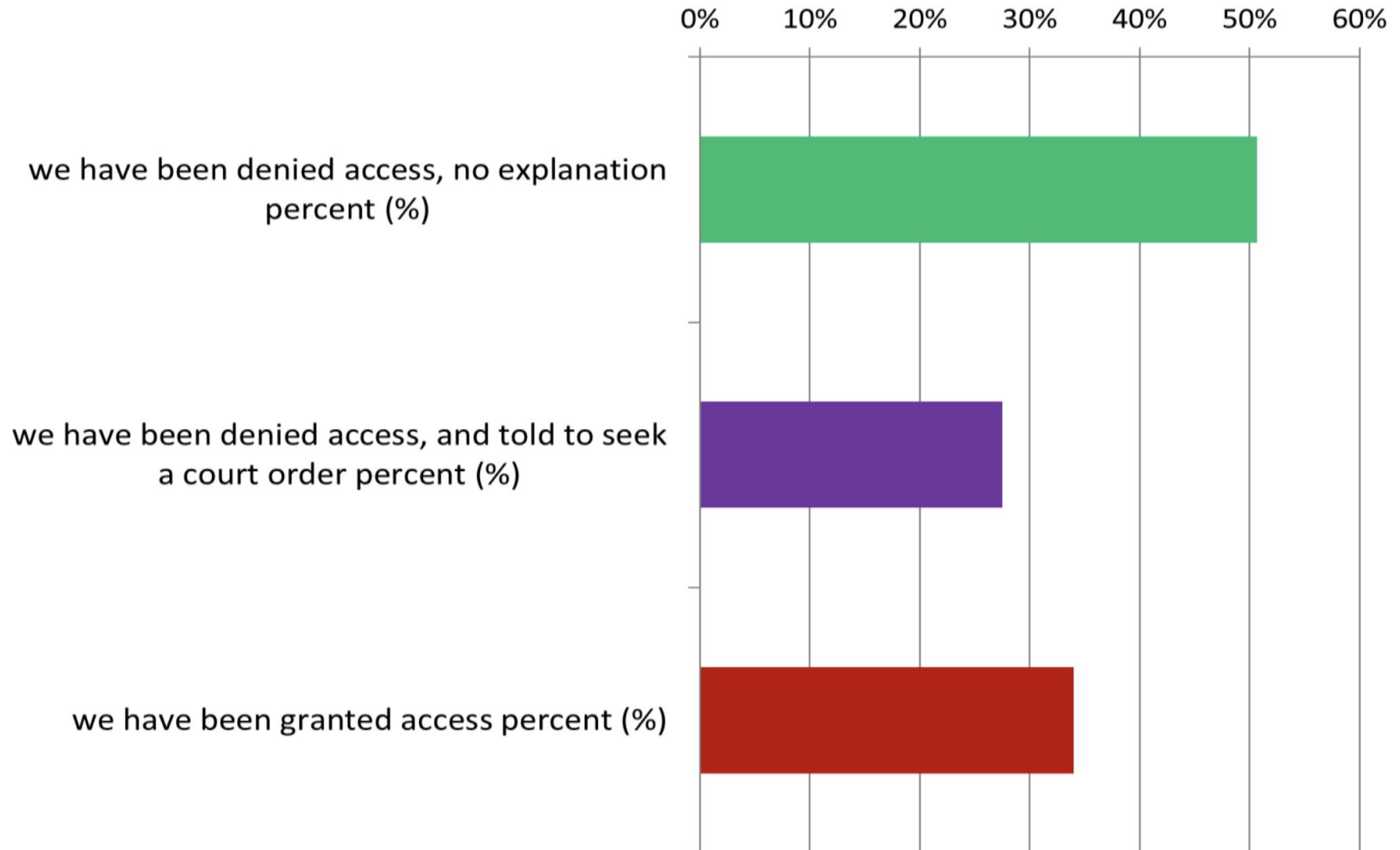


Though Whois contact data has been redacted for many domains since May 25, 2018, WHOIS users with legitimate and legal purposes may request access to redacted data. Have you submitted requests to reveal redacted WHOIS contact data?

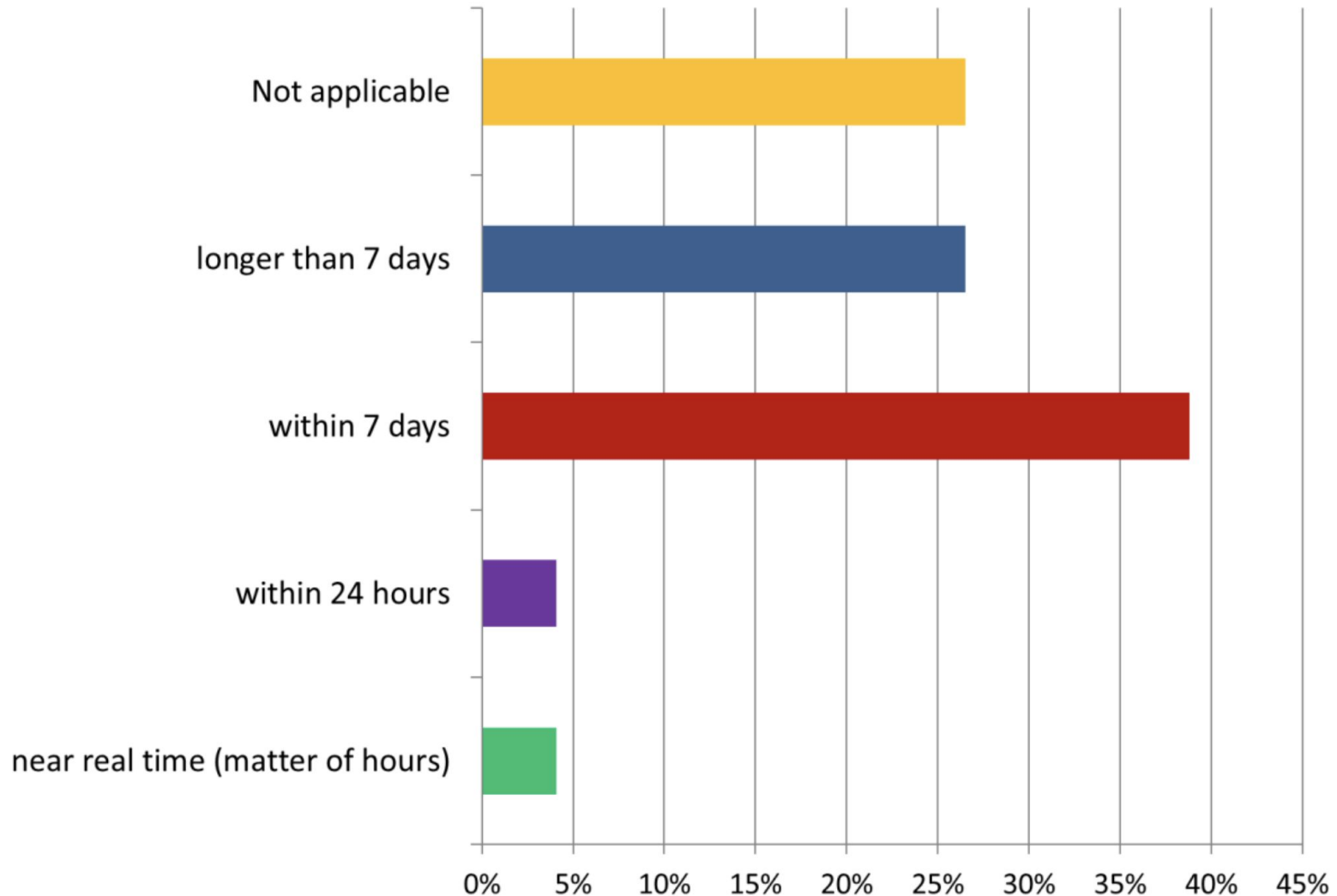


Source: ICANN GDPR and WHOIS Users [Survey](#), APWG & MAAWG, 18 October 2018

Describe your experience when requesting reveal of redacted data: (please estimate percent for each case, 1-100%, and make sure that the total of the three does not exceed 100)

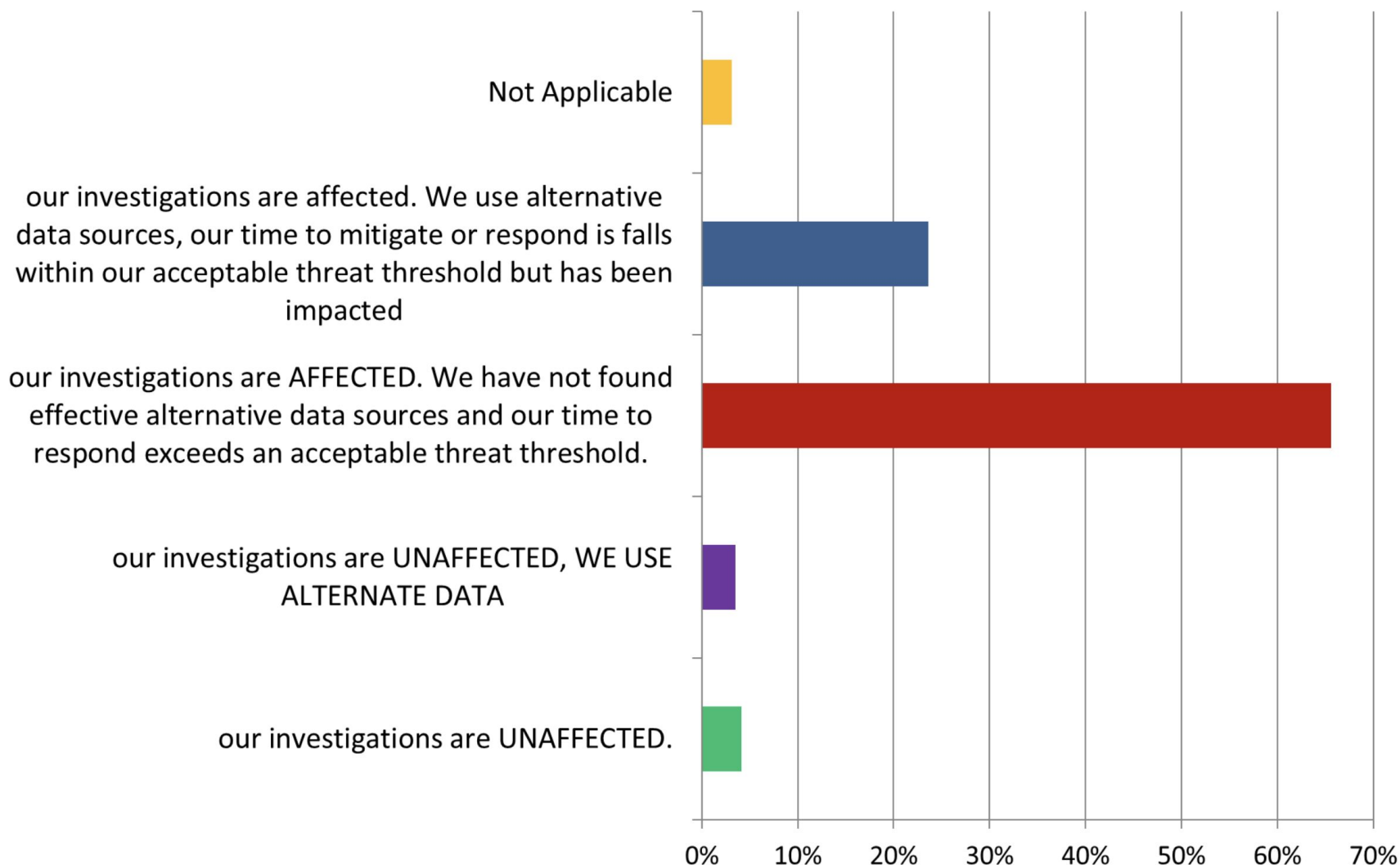


In circumstances where you are granted access to redacted data through reveal, what response times are you experiencing?

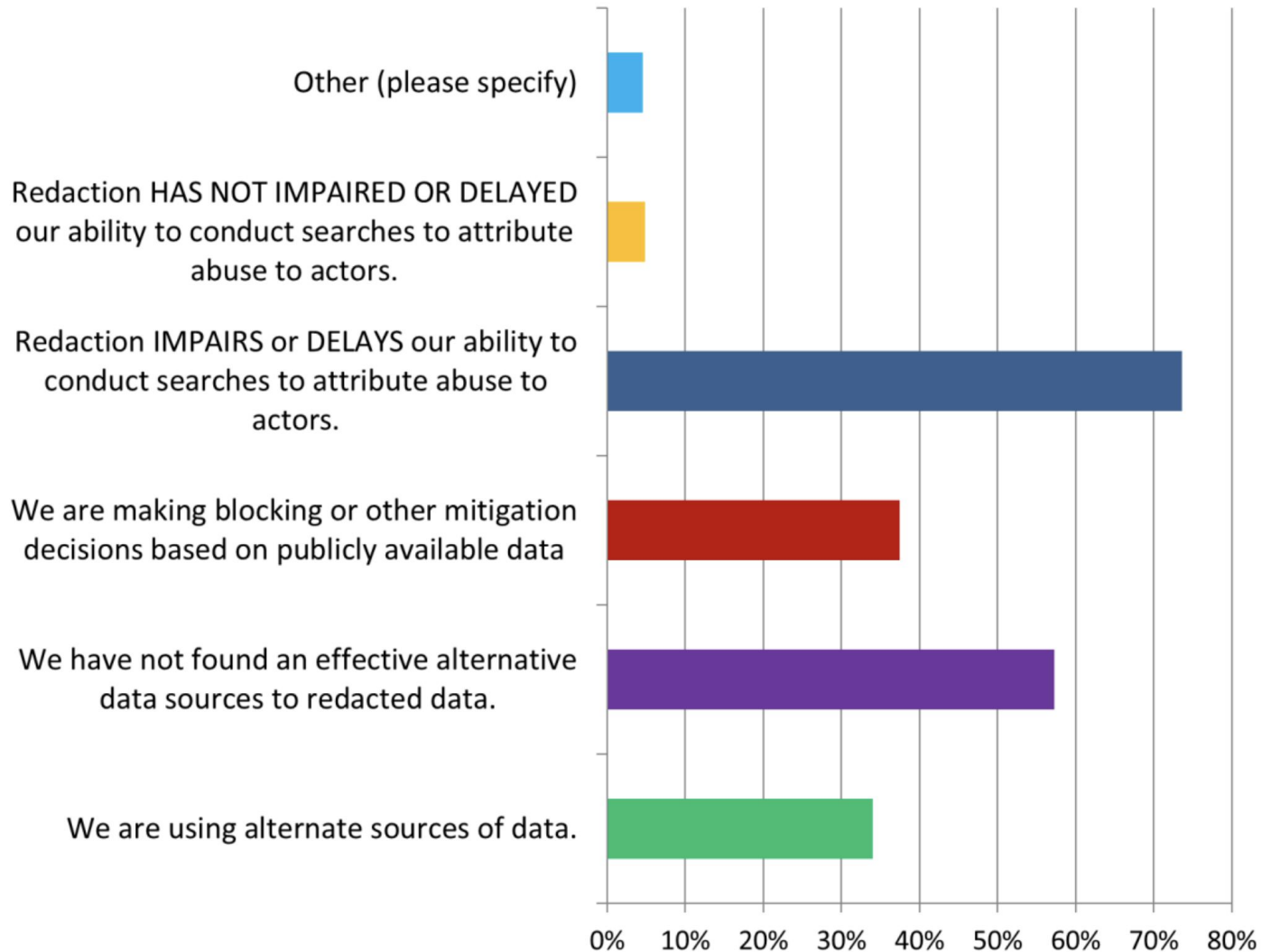


Source: ICANN GDPR and WHOIS Users [Survey](#), APWG & MAAWG, 18 October 2018

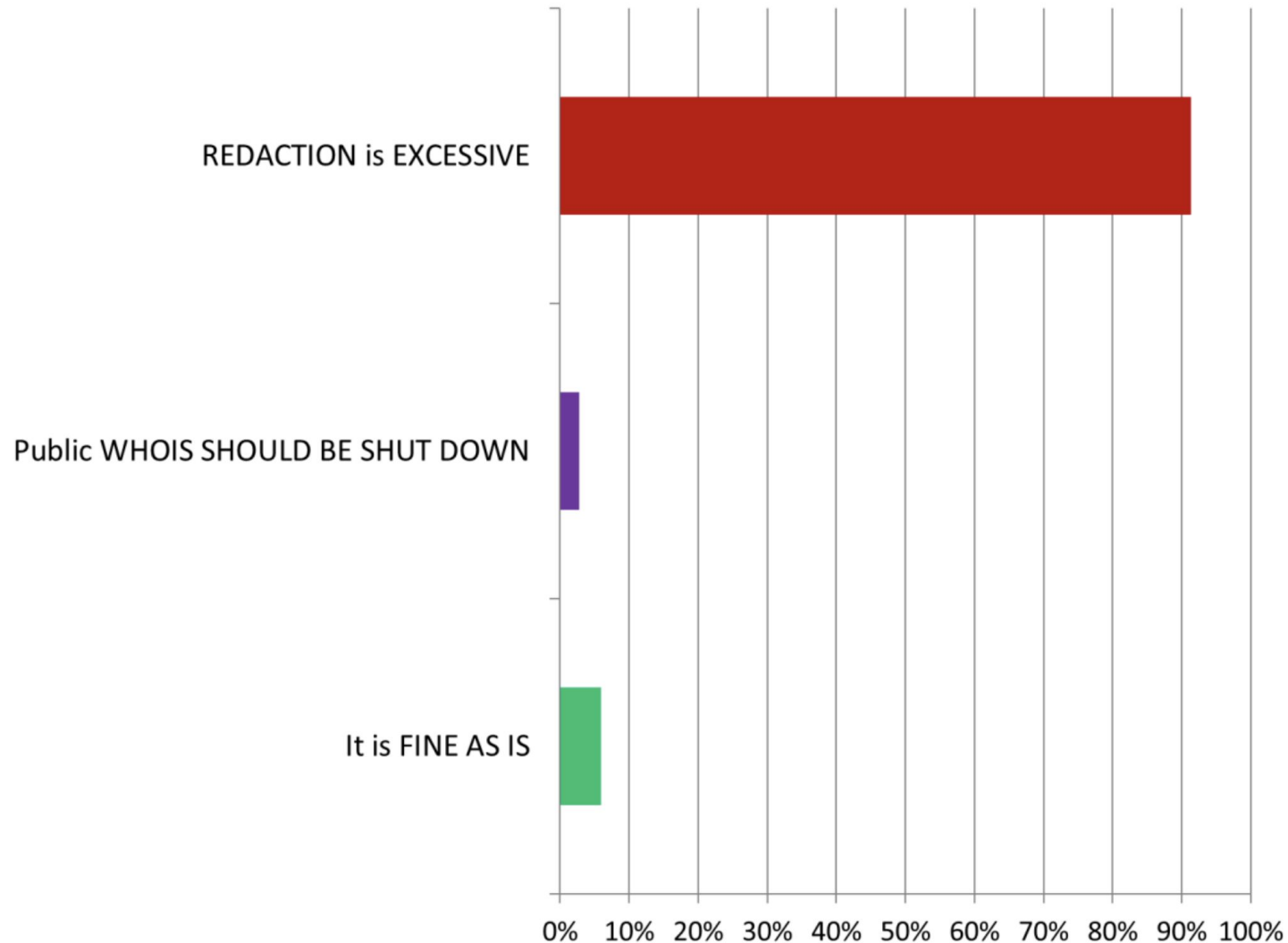
Which of these statements best matches how the changes introduced in the ICANN Temporary Specification for WHOIS have affected your investigations?



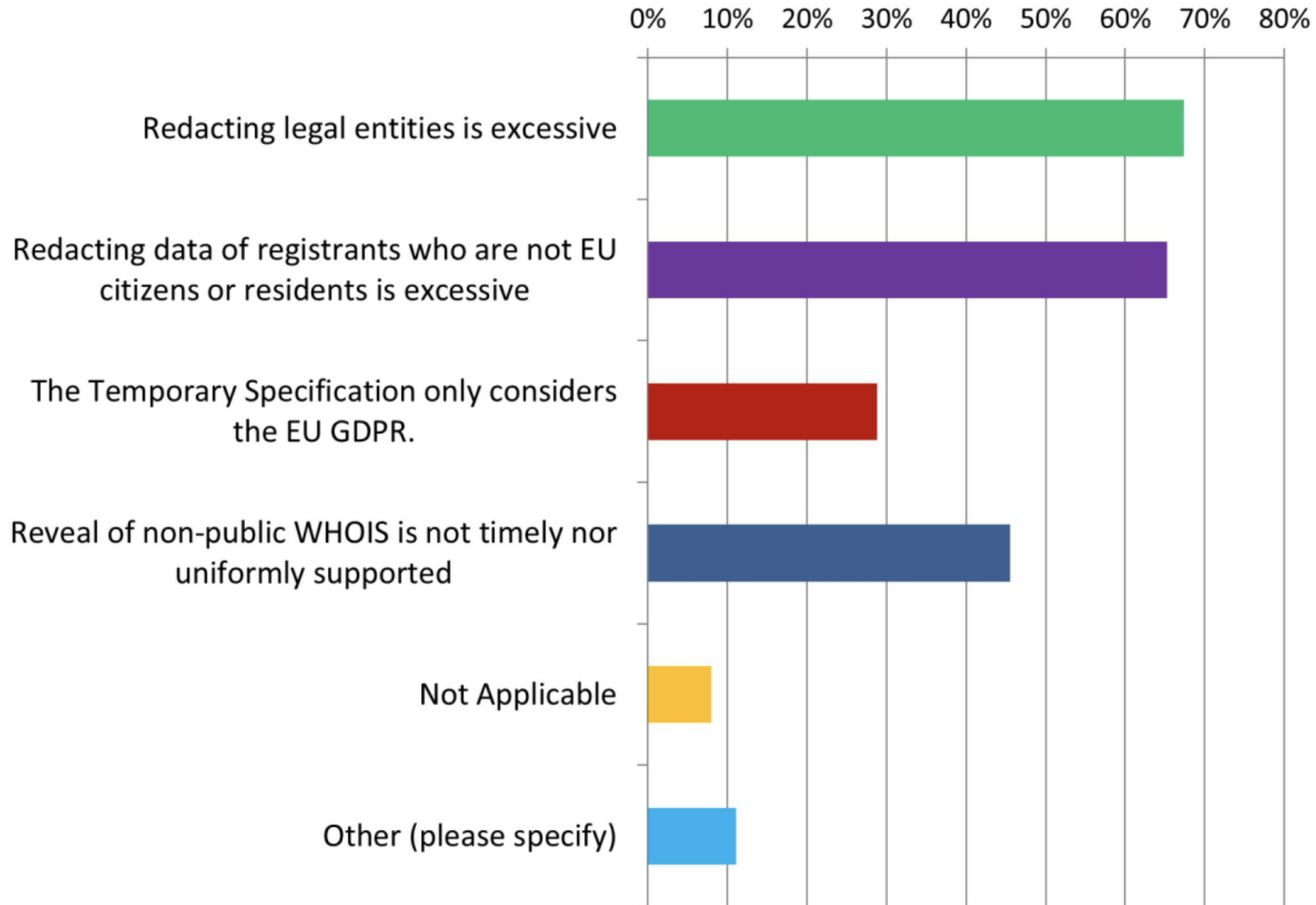
Which of these statements reflect your experience with the temporary spec for WHOIS: (Choose all that apply)



What if any issues do you have with how the temporary spec has altered WHOIS:



If you chose redaction is excessive in (Q11), please explain why: (Choose all that apply)



- Requests for non public data to registrars have inconsistent, unpredictable results
- Temporary specification is too vague regarding access to non public data
- Some registrars are not providing reasonable access by systematically requiring court orders
- Investigations take longer; victims at risk longer
- Not seeing the full impact on investigations yet:
 - LEA still have access to pre 25 May 2018 data
 - Nevertheless, ability to attribute crime is degrading

- Immediate access to non public data via central portal
- Reverse Lookup (Searchability of Whois)
- Historical Whois (Requires longer data retention)
- Single and multiple query capabilities
- Cybersecurity researchers' access to non public data (including reverse lookup)

1. Introduction and Review of PSWG Activities
2. WHOIS Compliance with GDPR: Impact of ICANN's Temporary Specification on Law Enforcement
3. DNS Abuse Mitigation: update on Domain Abuse Activity Reporting (DAAR) by ICANN (John Crain, ICANN)